Study Guide

FTEALMUN'25

GA:6 LEGAL STUDY GUIDE

UNDER SECRETARY GENERAL
Atahan Gider

ACADEMIC ASSISTANT
İdil Irmak Doğan

TABLE OF CONTENT

Letter from the Co-Secretaries-General

Letter from the Co-Secretaries-General

Distinguished Delegates of FTEALMUN'25,

It is a great honour to welcome you all to FTEALMUN’25. In an age when global challenges affect each of us more profoundly than ever before, this conference represents far more than a gathering of students. It is a space where young voices can question, connect, and take the first steps toward shaping lasting change. The committees and agendas have been crafted with care, each one designed to spark meaningful dialogue, challenge existing perspectives, and inspire innovative solutions to the world’s most pressing issues.

The true strength of FTEALMUN’25 lies in its diversity. Bringing together delegates from different backgrounds and viewpoints, this conference is a reminder that progress stems from the exchange of ideas. It is not only about policies or resolutions but about learning from one another, testing convictions, and building a community where every vision is valued. As you take on the role of diplomats, I encourage you to keep your minds open, to lead with patience and empathy, and to embrace the discomfort that often comes with meaningful negotiation.

I hope this experience empowers you to bring your full self into every discussion. Let it be a stepping stone in your journey to becoming thoughtful, forward-looking leaders. Each of you carries a unique perspective, and together you will define the spirit and success of this conference. My team and I are excited to see the passion, creativity, and determination you bring to the table.

On behalf of the entire Secretariat, thank you for joining us in this endeavour. May FTEALMUN’25 not only be remembered for its debates but also for the friendships formed, the lessons learned, and the inspiration that stays with us long after the final session concludes.

Warm regards,

Haktan Efe Özgür, Ela Çakır

Co-Secretaries-General of FTEALMUN’25

Letter from the Under Secretary-General

Hello, Honorable Delegates of FTEALMUN'25. My name is Atahan Gider, a senior student at Bahçeşehir Koleji, and I am ecstatic to be your Under-Secretary General of GA:6 LEGAL. I am fully aware that no one will read this. However, I would like to extend my gratitude to our Co-Secretaries General, Haktan Efe Özgür and Ela Çakır, for granting me this opportunity to serve as your Under-Secretary General. I would also like to thank my dear Academic Assistant, İdil Irmak Doğan, for helping me write this study guide. I would also like to extend my heartfelt thanks to the Committee Directors for their dedication and hard work.

As we gather here at FTEALMUN'25, we are not only stepping into a room to debate resolutions and draft clauses; we are stepping into the frontlines of one of the most defining challenges of our era—the governance of cyberspace. The world we live in today is interconnected in ways that our predecessors could only imagine. Our societies, economies, and even personal identities increasingly exist in digital form. Yet, while our data flows seamlessly across continents, the laws that govern this virtual world remain fragmented, ambiguous, and often contested. It is within this context that GA:6 LEGAL takes on a profound responsibility: to examine, define, and propose a framework for digital sovereignty and the legal status of online territories.

This agenda item is not merely about technical definitions or legal jargon. It is about the very balance between state sovereignty, individual freedoms, and international cooperation. It is about ensuring that nations can protect their citizens and infrastructure without eroding the freedoms, privacy, and human rights that form the foundation of modern democracies. As delegates, you will debate whether cyberspace should be treated as a neutral, global commons or whether it should reflect the boundaries, responsibilities, and rights of the physical world. You will grapple with questions of accountability, jurisdiction, and the role of multinational technology companies that hold power rivaling that of nation-states.

As we navigate these complex discussions, I urge you to remember the human dimension behind every clause and amendment. Every regulation on digital borders affects the daily lives of billions—students accessing online education, journalists safeguarding sources, doctors sharing

critical data, and ordinary citizens entrusting their privacy to platforms that operate across borders. Our decisions in this chamber, though framed in the language of law and policy, will echo far beyond these walls. They will shape the global understanding of cyberspace for years to come.

I encourage each of you to approach this agenda with both rigor and empathy, to question assumptions, and to seek solutions that balance innovation, security, and human dignity. Let us be bold yet thoughtful, principled yet pragmatic. This committee has the unique opportunity to chart the path forward, to define not only rules and norms but also the ethical compass that guides international cyber governance.

In closing, let us embrace this challenge with the seriousness it deserves, but also with the hope and optimism that meaningful cooperation is possible. May GA:6 LEGAL at FTEALMUN'25 be a forum where ideas transcend borders, where debates illuminate solutions, and where we collectively take one step closer to a cyberspace that is secure, open, and equitable for all.
Thank you, and I wish you all a productive, inspiring, and engaging conference.

Introduction to the Committee

The Sixth Committee of the United Nations General Assembly, also known as the Legal Committee, is the primary forum for considering legal matters within the UN framework. One of the General Assembly's six principal committees, it deals with issues regarding international law and cooperation between states in the law field. All UN Member States have the right to be represented in this committee, a fact that makes it one of the most universal legal debate forums in the world.

The Legal Committee is convened annually in New York during the regular session of the General Assembly, usually after the General Debate. In the course of these sessions, the

committee deals with a broad agenda of issues relating to the codification and progressive development of international law, the promotion of the rule of law and universal jurisdiction, the legal response to counter-terrorism, the status of diplomatic and consular relations, and the assurance of the protection of human rights by legal means.

One of the key functions of the Committee is to address emerging challenges of the international world by considering and establishing international law standards in line with the evolving political, technological, and social conditions of the international community. Its activity over recent years has introduced new, controversial issues such as cybersecurity, space law, climate liability, and the regulation of emerging technologies to its agenda.

With every advancing step of technology, the Sixth Committee stands at a crossroads, torn between the rapid pace of technological progress and the measured, incremental pace of international legal developments. It has to ensure that technology is used for human welfare without undermining the rights, security, or sovereignty of people and states. To delegates, it means grappling with new legal challenges and forging creative legal solutions that will stand the test of time, progress, and politics.

Definitions and Key Concepts

Digital Sovereignty

The right and capacity of a state to regulate, manage, and protect its digital infrastructure, data, and cyberspace activities within its jurisdiction—similar to physical sovereignty but applied to online environments.

Online Territories

Virtual spaces (servers, platforms, cloud regions, domains, or networks) treated as extensions of national jurisdiction or operating as quasi-territories in international law.

Jurisdiction in Cyberspace

The legal authority of a state to enforce laws on digital activities, infrastructure, or individuals, often categorized into territorial, personal, and extraterritorial jurisdiction.

Legal Frameworks

A legal framework consists of laws, regulations, treaties, court decisions, and institutional arrangements that guide behavior within and across states. Legal frameworks in the field of emerging technologies are needed to set obligations, develop standards, and provide enforcement mechanisms to ensure these technologies are developed and deployed ethically, securely, and in a manner consistent with international legal norms.

Cyber Governance

The systems, rules, and structures used by states, companies, and international bodies to regulate behavior, security, and rights in the digital realm.

Digital Borders

Technical and legal boundaries states create to control data flow, platform access, internet content, and cross-border cyber operations (e.g., firewalls, data localization laws).

Data Sovereignty

A principle stating that all digital data is subject to the laws of the country where it is located, stored, or processed.

Cybercrime & Extraterritorial Enforcement

Illegal actions conducted online which require cross-border cooperation for investigation and prosecution (e.g., ransomware, hacking, phishing).

Cloud Jurisdiction

How international law applies to cloud services, where data may be stored across multiple countries or non-physical “cloud regions,” complicating sovereignty claims.

Budapest Convention (Cybercrime Convention)

The Budapest Convention on Cybercrime, adopted by the EU Council in 2001, was the first and is still the only binding international treaty on cybercrime, as it addresses tackling serious situations, such as data interference, offenses related to child pornography and copyright, and computer-related forgery, by giving member states legal grounds to preserve electronic evidence, conduct search and seizure of digital data, etc. However, this convention still faced criticism for the lack of inclusion of privacy safeguards.

National / Sovereign Cloud

A state-controlled cloud infrastructure used to store sensitive data securely within national boundaries.

Digital Citizenship

Programs (like in Estonia) where states provide online identity and legal rights independent of physical residence.

Virtual Embassies

Online representations of states used for outreach, digital services, or public diplomacy—raising jurisdiction and recognition questions.

Introduction to the Agenda Item

The Legal Status of Online Territories: Establishing Digital Sovereignty in Cyberspace

Digital sovereignty, cyber sovereignty, technological sovereignty and data sovereignty refer to the ability to have control over your own digital destiny – the data, hardware and software that you rely on and create. Over the past decade, the rapid digitalization of global society has blurred the boundaries between physical territories and online spaces. As governments, corporations, and

individuals increasingly operate within digital ecosystems, the concept of "territory" has expanded beyond physical geography into the virtual realm. This shift has raised pressing legal questions regarding jurisdiction, ownership, data governance, and the role of states in cyberspace. The agenda item *"The Legal Status of Online Territories: Establishing Digital Sovereig*nty in Cyberspace" challenges the international community to reconsider traditional interpretations of sovereignty and territorial integrity in the context of cloud infrastructures, cross-border data flows, online platforms, and decentralized networks.

As states assert greater control over their digital environments, disputes over cyber operations, data localization, network access, and platform regulation have intensified. Digital sovereignty has become a concern for many policymakers who feel there is too much control ceded to too few places, too little choice in the tech market, and too much power in the hands of a small number of tech companies, who control massive amounts of data about their users. At the same time, the lack of clear, universally accepted international legal frameworks creates inconsistencies that can undermine human rights, economic development, and global cybersecurity. This agenda calls upon delegates to explore how international law can evolve to address the governance of online territories while promoting cooperation, accountability, and stability in cyberspace.

Background of the Agenda Item

Development of Internet & Creation of Cyberspace (1990s - 2000s)

Although the term "Cyberspace" was first used in science fiction novels in 1980s, it is now used for technology strategists, security professionals, governments, military and industry leaders and entrepreneurs to describe the domain of the global technology environment, commonly defined as standing for the global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems. Cyberspace is fundamentally dependent on technical advancement and innovation. All digital interactions in this space, including sending emails, visiting websites, and using social media are part of cyberspace.

While the term was created in the 1980s, initial foundations of “cyberspace” were created in the 1940s - 1960s, together with the creation of the first computers and networks, such as ARPANET, which may be considered one of the first precursors of the Internet. In the following years, specifically in the 1990s, cyberspace became part of people’s lives with technologies such as the World Wide Web by Tim Berners-Lee and personal computers. When WWW developed, the Internet emerged as a web of millions of computers around the world that provided access to information, started a global communication system, and became the world's largest market place.

In the 2000s, also known as “The Golden Era of Internet”, the internet further developed with the availability of e-commerce, electronic communities, social networks, and multimedia contents. This period also realized the fact that the digital domain has in fact become a part of people’s daily lives and indeed of business. The online world also had an effect on primary and advanced education with an immense influence on the curriculum and activities.

Emergence of Cybercrime & First Legal Frameworks

As cyberspace has expanded, concerns about cyber security, privacy, and the ethical use of digital technologies have also increased. People, as well as governments and organizations, have encountered questions connected to cybercriminals, personal data control, and the regulation of cyberspace.

Moving to the 21st century, the rise of popularity on social media, AI, and smartphones also created unprecedented challenges, such as misinformation, cybercrimes, privacy threats, and security concerns. The Budapest Convention on Cybercrime, adopted by the EU Council in 2001, was the first and is still the only binding international treaty on cybercrime, as it addresses tackling serious situations, such as data interference, offenses related to child pornography and copyright, and computer-related forgery, by giving member states legal grounds to preserve electronic evidence, conduct search and seizure of digital data, etc. However, this convention still faced criticism for the lack of inclusion of privacy safeguards and did not define “online territories” or establish regulations regarding digital sovereignty.

Strengthening State Control & Online Borders (2010s)

As the internet became a vital instrument for national security, privacy, communication, education, and economic infrastructure, governments began to claim greater legal authority over digital spaces.

Starting off with China's approach to sovereignty, the development of a censor-system, called "the Great Firewall" in reference to the Great Wall of China. It is a combination of technological and legal regulation of the internet in China and it is a part of the "Golden Shield Project" deployed by the Chinese E-government. The Firewall has other effects as well, so by blocking companies from abroad, they are strengthening the development of national companies, for instance. The functioning of the firewall is quite easy to understand. Before being publicly accessible through the Chinese Internet, new domains must receive official approval. Similar to the Great Wall of China at the time, the Great Firewall allows the Chinese government to regulate both incoming and departing virtual data. The firewall consists of two separate programs: one that automatically filters questionable references and another that filters all restricted websites from the internet outside of China. Today, the government employs at least 50,000 individuals to implement the censorship, prohibiting websites it deems objectionable and compelling search engines to remove content deemed damaging. Additionally, an estimated 500 million pro-government comments are posted annually by an army of social media experts.

The Russian Federation has also latched on to digital sovereignty, creating "The Sovereign Internet Law" in 2019. The Sovereign Internet Law is the informal name for a set of 2019 amendments to existing Russian legislation that mandate Internet surveillance and grants the Russian government powers to partition Russia from the rest of the Internet, including the creation of a national fork of the Domain Name System (DNS). The country has over 5000 networks, several of which get address space directly from the regional European Internet registry–the RIPE NCC. This means they can switch transit providers more easily and they have autonomy over their choices, more than the networks in China, for example. Under the 'Sovereign Internet' law, however, every operator must send network schematics to Roskomnadzor, the government entity in charge of monitoring, controlling, and censoring mass media. They need to provide the regulator with technical characteristics of the communications

facilities where “technical means of countering threats” (TMCT) will be installed. This has an impact on communication channel data, such as the number, physical properties, loads, and locations of proposed installations. Operators will be forced to install Roskomnadzor's TMCT on their systems and regularly give precise routing information to the regulator. They will also need to grant Roskomnadzor remote access to the TMCT.

Apart from individual nations, the European Union has set the international basis for data protection and safety. The General Data Protection Regulation (GDPR) is EU legislation that came into effect on May 25, 2018. It has wide-reaching implications for data protection and security. GDPR applies to any organization that operates within the European Union (EU), as well as organizations that provide products or services to EU people, regardless of location. Under the GDPR, organizations must gain explicit consent to collect, use, or process personal data. They also need a lawful basis for processing the data — such as a contract with the individual or a legitimate interest in processing the data. This gives EU residents much more control over personal data, or data that can be used to identify them. While the GDPR does not specifically mention cloud storage, it does apply when a company is processing personal data in the cloud.

Current International Legal Frameworks

As traditional rules were created for physical regions rather than virtual ones, the international legal framework governing cyberspace is still fragmented. While a number of treaties, norms, and principles address some aspects of cyber governance, none offer a thorough description of "online territories" or create widely recognized guidelines for digital sovereignty. States' differing interpretations of their rights and responsibilities result in overlapping jurisdictions, uneven enforcement, and legal ambiguity.

Numerous UN authorities have confirmed that international law does apply to cyberspace; yet, it is difficult to apply ideas like territoriality, sovereignty, jurisdiction, and state accountability to a domain that is decentralized, borderless, and primarily controlled by private parties. Therefore,

rather than relying on legally binding international regulations, the current framework mostly relies on soft law, political agreements, and voluntary collaboration.

Existing Treaties and Conventions (International & Regional)

1. **Budapest Convention on Cybercrime (2001)**

   As this convention was mentioned above, the Budapest Convention is the most important international pact on cybercrime and cross-border digital investigations. It creates protocols for evidence exchange, jurisdiction, and cooperation. However, it does not define online territories or governs state sovereignty in cyberspace. Several significant countries, including China and Russia, are not signatories to the convention, restricting its universality.

2. **International Covenant on Civil and Political Rights (ICCPR)**

   The International Covenant on Civil and Political Rights (ICCPR) is a key human rights treaty that protects fundamental freedoms and civil liberties, ensuring individuals' rights to life, freedom of speech, fair trials, privacy, and protection from torture, arbitrary detention, and discrimination. Although not cyber-specific, the ICCPR regulates online rights such as privacy, freedom of expression, and data protection. States must adhere to these duties even when pursuing digital sovereignty or content regulation.

3. **African Union Convention on Cyber Security (Malabo Convention)**

   The African Union Convention on Cyber Security and Personal Data Protection also known as the Malabo Convention is a 2014 legal framework adopted by the African Union (AU) to address cybercrime and data protection in Africa. The Convention outlines unified guidelines and regulations for different aspects of e-commerce, such as online advertising, the legal recognition of electronic contracts, and securing electronic payment systems. The Malabo Convention criminalizes different cyber activities and obliges each member state to create a national cybersecurity policy and strategy. It also advocates for the establishment of appropriate institutions and processes to detect and

resolve cybersecurity risks, uphold important cybersecurity ideals, and promote international collaboration. Further details can be found on this link or in the Bibliography Section.

4. General Data Protection Regulation (GDPR)

The GDPR significantly impacts data sovereignty by enforcing strict guidelines on data handling and storage within the EU. Organizations must ensure that personal data remains within the jurisdiction of the EU or is transferred only to countries with equivalent data protection standards. GDPR mandates explicit consent for data collection, clear data usage policies, and the right for individuals to access, correct, or delete their data. Data sovereignty under GDPR emphasizes that data protection laws apply based on the location of the data subject, not the data processor. Companies must implement security measures, such as encryption and access controls. It also includes provisions for cross-border data transfers, requiring organizations to use mechanisms like Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) to ensure compliance.

5. ASEAN Digital Masterplan

The ASEAN Digital Masterplan is a regional strategic framework created by the Association of Southeast Asian Nations (ASEAN) to support digital transformation, cybersecurity, connectivity, and economic integration across Southeast Asia. As one of the most populous and diverse regions in the world, ASEAN is set to become a top five digital economy by 2025. ASEAN's digital ambition has been put forth in the ASEAN Digital Masterplan 2025, which promotes "ASEAN as a leading digital community and economic bloc, powered by secure and transformative digital services, technologies, and ecosystem." It supports regional norms for data protection, sovereignty, and cross-border data governance and contributes to coordinated cyber policy among Southeast Asian states.

6. National Digital Sovereignty Laws

Countries such as China, Russia, India, and Saudi Arabia have enacted strict digital sovereignty laws, but they function independently rather than under a common legal regime. This creates a global patchwork rather than a unified system.

Role of the United Nations and International Bodies

1. UN Group of Governmental Experts (UN GGE)

The UN Group of Governmental Experts (UN GGE) is a specialized UN body composed of a small group of selected member states appointed by the UN Secretary-General to study and develop norms on international cybersecurity. UN GGE encourages transparency and confidence-building measures to reduce cyber conflict. The GGE has played a central role in shaping norms around responsible state behavior in cyberspace. Its reports (2013, 2015, 2021) confirmed that: international law applies to cyberspace, states should not target critical civilian infrastructure, states must cooperate to prevent malicious cyber activities. However, the GGE did not establish rules defining online territories or limiting digital sovereignty claims.

2. Open-Ended Working Group (OEWG)

The Open-ended Working Group (OEWG), one of the subsidiary bodies of the Basel Convention, was given the following mandate by decision VI/36 (Institutional arrangements), adopted by the sixth meeting of the Conference of the Parties (COP) to the Basel Convention. The OEWG is tasked with studying existing and potential threats in the sphere of information security, including data security to promote common understandings. The OEWG also emphasizes confidence-building measures and capacity-building initiatives to enhance collective cybersecurity.

3. International Telecommunication Union (ITU)

ITU is the United Nations specialized agency for digital technologies (ICTs). The Organization is made up of a membership of 194 Member States and more than 1000

companies, universities and international and regional organizations. ITU facilitates international connectivity in communication networks and allocates global radio spectrum and satellite orbits, develops the technical standards that ensure networks and technologies connect seamlessly, and works to improve access to digital technologies in underserved communities worldwide. The ITU has developed an extensive program on cybersecurity. Three activities are particularly relevant for promoting accountability in cyberspace: the Global Cybersecurity Index, National Cybersecurity Strategies, and the National CIRT program. To provide countries with a clear framework for developing their national strategies, the ITU led a group of 25 organizations in developing a Guide to Developing an NCS, currently in its second edition. The NCS guide forms the basis for ITU's BDT and the work of other implementing organizations when supporting countries' efforts to develop or update their national cybersecurity strategies.

4. International Court of Justice (ICJ)

The International Court of Justice or or colloquially the World Court, is the principal judicial organ of the United Nations (UN). It settles legal disputes submitted to it by states and provides advisory opinions on legal questions referred to it by other UN organs and specialized agencies. The ICJ is the only international court that adjudicates general disputes between countries, with its rulings and opinions serving as primary sources of international law. It is one of the six principal organs of the United Nations. The ICJ has not yet ruled on cases involving digital sovereignty or cyber territorial disputes. However, principles of state responsibility and jurisdiction could be extended to future cyber-related cases.

5. North Atlantic Treaty Organization (NATO)

NATO's purpose is to guarantee the freedom and security of its members through political and military means. NATO promotes democratic values and provides a permanent structure for its members to consult and cooperate on defence and security-related issues and committed to the peaceful resolution of disputes. However, if diplomatic efforts fail, it has the military power needed to defend every one of its members – as stated in Article 5, the collective defence clause of NATO's founding treaty.

NATO recognizes cyberspace as an operational domain and supports collective cybersecurity.

Challenges & Concerns

The debate on digital sovereignty and the legal status of online territories is shaped by multiple political, technical, and human rights challenges. While states attempt to protect their digital infrastructure and assert control over data flows, such efforts often clash with principles of global connectivity, privacy rights, platform neutrality, and international cooperation. Many governments seek stronger digital borders to enhance national security, yet doing so can trigger censorship, surveillance, and internet fragmentation. At the same time, rising cybercrime, geopolitical tensions, and the involvement of powerful private companies complicate the creation of a unified legal framework.

The controversies surrounding the agenda item stem from the difficulty of balancing three priorities: state sovereignty, global interoperability, and individual rights. Without consensus on how international law should apply in cyberspace, states frequently adopt conflicting digital policies, leading to uncertainty and legal grey zones.

Data Privacy, Security, and Human Rights Concerns

1. **Data Privacy Conflicts**

   Digital sovereignty and data privacy are not mutually exclusive; instead, they are complementary approaches to data protection. Digital sovereignty provides the legal and policy framework for controlling data, while data privacy focuses on protecting data in use, while using technical controls to enforce, mitigate risk, and ensure compliance, even when data is being processed, that is while data is in use.

As states enforce digital sovereignty through data localization, cloud regulations, and surveillance measures, concerns rise over the protection of personal data. Some governments justify strict control over data flows as a way to ensure national security.

The importance of data privacy will only continue to escalate. New and evolving data privacy regulations are constantly being introduced worldwide, reflecting a growing recognition of the value of data and the need to protect individual rights. Simultaneously, cyberattacks are becoming more sophisticated, with malicious actors constantly seeking new ways to exploit vulnerabilities and steal sensitive information. Furthermore, there is a growing public awareness and concern about data privacy, with individuals demanding greater control over their personal information.

Digital sovereignty, confidential computing and protecting data in use will become increasingly essential for organizations in this context. Organizations prioritizing these concepts will be better positioned to maintain a competitive advantage by building customer trust, ensuring long-term compliance, and avoiding costly penalties. Moreover, these technologies will enable organizations to foster innovation while safeguarding sensitive information, allowing them to explore new opportunities without compromising privacy.

2. Security Concerns

Data sovereignty can increase cybersecurity risks, particularly if data is stored in a single location or jurisdiction. This can make it easier for cybercriminals to target and compromise data, which can have significant financial and reputational consequences for businesses.

Efforts to secure digital territories often require monitoring online activities, restricting content, or blocking foreign platforms. These measures raise questions such as:

- How much state control is necessary for security?
- Where is the line between legitimate regulation and censorship?

- Can digital sovereignty be exercised without undermining democratic freedoms?

Countries with strong cybersecurity laws argue that strict governance is essential, while civil society groups warn that such models can be misused to justify repression.

3. Human Rights Implications

Technological advancement results in new business models and ways to connect, learn, create, and participate in civic spaces and the economy. It brings challenges such as breaches of privacy and the spread of illegal and harmful content online, which can diminish trust in governments and the digital environment, and undermine democratic principles. At the same time, broad and equitable access to the Internet and digital tools is essential for education, work and social engagement.

The digital age creates novel avenues for people to exercise and enjoy their rights, but also new ways in which they can be infringed. At the same time, governments and stakeholders have raised questions regarding the protection of interests unique to the digital context (such as Internet access), including whether such interests should be protected as rights, and what such protections would entail. In contributing to this conversation, it is helpful to ask:

- Does digital transformation change traditional expectations of how governments can uphold and protect rights in the digital age?
- Do digital technologies compound the balancing act necessary when faced with tensions between human rights?

4. Effects on Businesses

Digital sovereignty is not merely a matter of compliance or cybersecurity. At its core, it's about strategic autonomy. Today, over 90% of Western data is stored or processed through cloud infrastructures owned by U.S. tech giants like Amazon Web Services, Microsoft Azure, and Google Cloud. According to an April 2025 CIGREF study, 80% of

Europe's professional cloud and software spending—amounting to €265 billion—is captured by American providers.

This structural dependency exposes European firms to significant vulnerabilities. In the event of geopolitical tensions, Washington could tighten controls on sensitive technologies, as it did with China in October 2023. This could lead to usage restrictions or sudden price hikes for European clients.

Moreover, U.S. laws like the Cloud Act allow American authorities to compel domestic companies to hand over data stored abroad. This extraterritorial reach adds a layer of legal uncertainty. And then there's vendor lock-in: the technological stranglehold that makes switching providers prohibitively expensive and operationally risky.

Instances of Cybercrime

Cybercrime remains one of the most serious catalysts pushing states toward stronger digital sovereignty. The borderless nature of the internet allows malicious actors to operate across jurisdictions, making traditional law enforcement tools ineffective. Key types of cybercrime relevant to this agenda include:

1. **Ransomware Attacks**

   Criminal groups increasingly target hospitals, government agencies, energy systems, and private companies. Ransomware gangs often operate from states with weak cybercrime laws or limited cooperation with international authorities, highlighting the need for cross-border legal frameworks.

2. **Financial and Identity Theft**

   Phishing schemes, credit card fraud, crypto-scams, and identity theft affect millions of users globally. The anonymity of online spaces and the use of decentralized networks make it difficult to track perpetrators.

3. State-Sponsored Cyber Operations

Though not always classified as "cybercrime," state-linked cyber operations against critical infrastructure raise severe legal controversies. Examples include:

- Attacks on election systems
- Espionage targeting government networks
- Sabotage of power grids or communication systems

These incidents challenge the existing interpretation of sovereignty, as they blur the line between criminal activity and acts attributable to states.

4. Darknet Markets and Illegal Trade

Drugs, weapons, malware tools, and stolen data circulate through encrypted online marketplaces. These networks operate beyond normal territorial law enforcement and require clear international rules to investigate and prosecute offenders.

5. Child Exploitation and Online Abuse

One of the most urgent areas of cybercrime involves the distribution of illegal content through encrypted or hidden online environments. Cooperation between states is essential, yet conflicting digital sovereignty laws often slow down investigations.

Case Studies

Case studies help illustrate how states across the world interpret digital sovereignty and apply control over online territories in different ways. These examples reflect the diversity of approaches and highlight the legal challenges posed by rapidly evolving digital ecosystems. Since we have gone through Russia's, China's, and European Union's established cyber sovereignty and regulations, other regional and international regulations will be presented in this segment.

1. United States - Cloud Act & Corporate Jurisdiction

The U.S. Cloud Act (2018) allows American law enforcement to request data stored abroad from U.S.-based cloud providers. This sparked global concerns about extraterritorial jurisdiction and foreign data exposure. The Microsoft Ireland Case, in which U.S. authorities sought data stored in an Irish server, highlights the legal complexities of cloud-based "territory."

2. Estonia - Digital Nation and E-Residency

Estonia is a pioneer in digital governance, offering e-residency, digital ID systems, and online public services. Estonia treats digital infrastructure as a core component of national identity and resilience. Its approach shows how small states can leverage digital territory to enhance economic development and cybersecurity. One of the main benefits of Estonia's e-Residency program is that it allows you to start a business in the country from anywhere in the world. You can run your business using Estonian financial services, which have been ranked by Transparency International among the most transparent and reliable in Europe. Estonia has a well-developed network of digital identity providers, so it's easy for e-residents to verify their identities online without having to physically visit an embassy or consulate for identification documents.

3. India - Data Localization and Platform Regulation

India introduced strong data localization requirements and compelled major tech companies to store sensitive data inside the country. This reflects a rising trend among developing economies to assert digital sovereignty to protect national security. However, critics argue such measures risk creating compliance burdens and limiting global data exchange.

4. Singapore - Cybersecurity as National Infrastructure

Singapore's Cybersecurity Act treats digital systems as critical infrastructure, giving the state authority to regulate private-sector networks. Its model emphasizes national security and public safety, often cited as a balanced, efficient approach to digital sovereignty without extensive censorship.

Role of Tech Giants and Companies

Tech corporations hold enormous influence in cyberspace—often more than many national governments. As the primary operators of cloud infrastructure, social media platforms, search engines, and digital communication systems, these companies shape global digital norms and control vast "online territories" that users depend on every day.

Control over Digital Infrastructure

Firms such as Amazon Web Services (AWS), Google Cloud, Microsoft Azure, Cloudflare, and Alibaba Cloud operate global data centers that store government and corporate data across multiple jurisdictions. However, it fails to address key elements such as, the person/group who controls the data, companies' cooperation with governments or third-party entities, who is taken responsible for security breaches, or how national laws apply to decentralized server networks.

Platform Governance and Moderation

Social media giants (Meta, X/Twitter, TikTok), messaging apps (WhatsApp, Telegram), and content platforms (YouTube, Reddit) govern massive online spaces. Free speech, disinformation, privacy, user security, national elections, propaganda, and advertisements can be affected by the platform's policies and regulations. When platforms block content or accounts, they effectively exercise sovereign-like power over digital communities.

Conflicts Between Corporate Policies and State Laws

States often require companies to:

- Remove content (censorship orders)
- Share user data for investigations
- Store data locally
- Restrict foreign influence or advertisements

Companies must choose between obeying local laws or global policies, leading to tensions—as seen with:

- Prohibition or suspension of "TikTok" in multiple countries

- Apple refusing to unlock iPhones for the FBI
- Meta and the EU fighting over data transfer rules
- Huawei's Infrastructure deployment (5G) and geopolitical security concerns.
- OpenAI's Influence in global AI safety, data use, and emerging digital governance models.
- China's digital governance, censorship, and data ecosystem regulated by Tencent & Alibaba.
- Türkiye demanded removal of political content; Twitter complied during elections, raising concerns about censorship vs. sovereignty; demonstrates how states alter platform governance
- Discord's successful cooperation in youth protection and investigations with countries such as Brazil and the United States but refusal with Türkiye; ultimately leading to a ban.

These conflicts reflect the overlapping sovereignties of states and corporations.

Country Stances

United States of America

The United States champions an open, global, and interoperable cyberspace that minimizes strict digital borders and avoids excessive government control. Washington prioritizes the free flow of data, opposes mandatory data localization, and strongly favors a multi-stakeholder governance model where private companies, civil society, and technical organizations collectively shape internet policy. The U.S. maintains that human rights, privacy, and freedom of expression must remain central to digital governance.

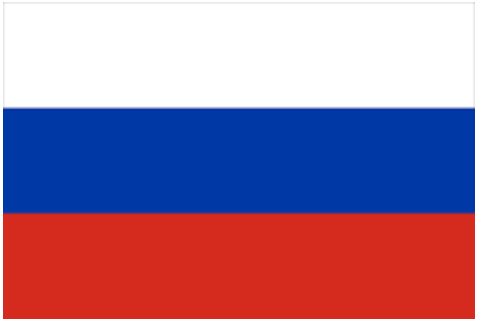
At the same time, the United States seeks to advance voluntary international cyber norms rather than binding global treaties that could restrict U.S. technological leadership or limit

private-sector innovation. The U.S. strongly supports norms against state-sponsored cyberattacks and pushes for cooperation on cyber defense, but retains strategic flexibility in how digital sovereignty is legally defined.

Estonia

Estonia is widely recognized as one of the most digitally advanced states and a global leader in cyber governance. After experiencing a nationwide cyberattack in 2007, Estonia argues that cyber operations can constitute violations of sovereignty and even trigger collective defense obligations under Article 5 of the NATO Treaty. The country strongly supports formal recognition of cyber threats within international law and advocates for transparency, accountability, and firm international norms for cyberspace behavior.

Estonia promotes an open, secure, and rights-protecting internet, rejecting heavily restricted digital models. It also supports the creation of an international cyber attribution system and frameworks that help smaller states enhance their cybersecurity and digital governance capacities.



Russia

Russia promotes a model of cyberspace rooted in strong state control and absolute national sovereignty over all online information operating within its borders. Moscow seeks to formalize this approach through a comprehensive, legally binding UN cyber treaty that grants states the authority to regulate content, control infrastructure, and monitor data flows domestically. Russia

positions digital sovereignty as essential for protecting national security and preventing foreign political influence.

Russia opposes Western-led, multi-stakeholder internet governance bodies, especially those based in the United States. Instead, it advocates for a state-centric model where governments, not private companies, hold decision-making power over digital territory, infrastructure, and information. This stance places Russia at the core of the global "cyber-sovereignty" bloc alongside China.

China

China is a leading advocate of strong digital territoriality, embodied in its Great Firewall, Cybersecurity Law, and extensive regulatory oversight of online platforms. Beijing argues that states should have absolute sovereignty over their digital spaces, including full authority over data, content, platforms, algorithms, and cross-border information flows. China seeks to enshrine this model in international law, promoting the idea that cyberspace is an extension of physical territory and national jurisdiction.

China favors a governance model dominated by states rather than private companies or NGOs and emphasizes "cyber stability" and "content security." Critics argue this approach reinforces censorship and surveillance, but China frames it as necessary for national security, social harmony, and digital independence. China also expands its influence through global digital infrastructure projects such as Huawei and cloud computing networks.

Türkiye

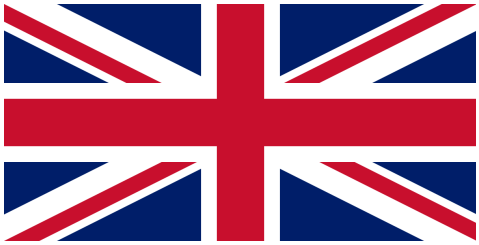
Türkiye supports a balanced approach to digital sovereignty—emphasizing national control, platform regulation, and strong cybersecurity measures, while still valuing international cooperation. The country focuses heavily on combating disinformation, protecting critical infrastructure, and developing domestic digital capabilities. Türkiye has strengthened its regulatory framework on social media companies, data protection, and cross-border data flows, positioning itself between Western openness and Eastern state-centric models.

Türkiye advocates for clearer definitions of cybercrime, digital borders, and online jurisdiction at the international level. It supports frameworks that protect states' digital autonomy without undermining human rights or economic development. Türkiye promotes a pragmatic stance that combines national security priorities with engagement in global and regional digital governance institutions.

Germany

Germany is a strong proponent of a rules-based, human-rights-focused approach to cyberspace governance. As a key EU member, Germany supports GDPR, digital autonomy initiatives, and stricter oversight of major tech companies. Berlin advocates for strong privacy protections, secure data infrastructure, and robust enforcement of cyber norms. Germany believes international law applies fully to cyberspace and supports mechanisms to ensure accountability for cyberattacks and malicious online activity.

At the same time, Germany supports multilateral cooperation and encourages global alignment on technical standards, cybersecurity practices, and data governance principles. While open to binding international agreements, Germany insists that such agreements must protect individual rights, avoid authoritarian controls, and align with democratic values.

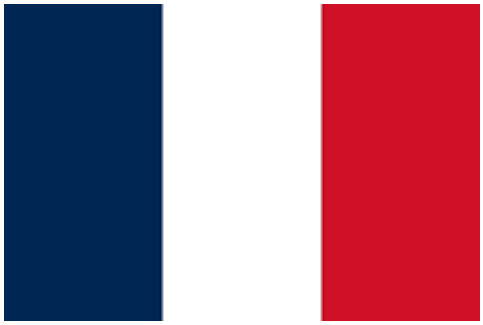


United Kingdom

The United Kingdom supports a free, open, and secure internet that emphasizes democratic governance, privacy,

and responsible state behavior. The UK opposes rigid digital borders or centralized state control over online content and infrastructure, arguing that such models undermine rights and inhibit economic innovation. It prioritizes combating state-sponsored cyber threats—particularly from Russia, China, and other adversarial actors—while supporting strong cybersecurity partnerships through NATO and the Commonwealth.

The UK favors international norms and transparency mechanisms but remains cautious about global cyber treaties that could restrict operational flexibility or impose disproportionate obligations on democratic states. Britain emphasizes cooperation with private-sector actors and supports frameworks that protect both national security and digital freedoms.



France

France advocates for strategic digital autonomy and greater European independence in data, cloud services, and cybersecurity. Paris supports defining clear rules for digital borders, critical infrastructure protection, and platform responsibilities. It strongly emphasizes human rights and data privacy while promoting frameworks that regulate the influence of large tech companies. France seeks a balanced approach that both recognizes state sovereignty and protects individual freedoms.

France supports binding legal norms and greater international cooperation but insists that countries retain the capacity to implement their own digital regulations within democratic boundaries. It favors a structured, treaty-based approach to cyberspace governance, provided it remains compatible with EU standards and fundamental freedoms.

Netherlands

The Netherlands strongly champions internet freedom, open data flows, and human rights online. As home to major internet infrastructure hubs, the Netherlands

supports a secure global internet but opposes digital fragmentation or heavy-handed state control. It believes that cyberspace governance should be shared among governments, private companies, and civil society rather than dictated by states alone.

The Netherlands emphasizes transparency in cyber operations, international accountability for malicious actions, and cooperation among democratic states to strengthen cybersecurity. It rejects authoritarian internet models and advocates for a digital environment that promotes innovation, connectivity, and fundamental rights.

Conclusion & Future Directions

The legal status of online territories and the concept of digital sovereignty remain among the most pressing and complex issues in contemporary international law. As states increasingly assert control over their digital spaces through laws, regulations, and technological infrastructure, the global community faces a tension between national sovereignty, international cooperation, and individual rights. The current international framework—comprising treaties, soft law, and regional regulations—offers important guidance but lacks universally binding norms for cyberspace. This gap has led to conflicting national policies, uneven enforcement, and a patchwork of regulations that complicate cross-border data flows, cybersecurity cooperation, and human rights protection.

Digital sovereignty is a notion emerged in the EU in relation to a specific series of initiatives. However, this chapter has shown that this concept can be used as a lens to interpret a broader phenomenon. As illustrated in the first part of this chapter, historically, the notion of sovereignty has denoted the power of the state over a territory and its independence from external actors. The advent of digital technology has accelerated the transition towards a global society where national boundaries are no longer neatly demarcated. This chapter has argued that in this post-territorial ecosystem the concept of sovereignty loses its traditional anchoring to the notion of territory. The physical location of a juridical entity becomes one of the various mechanisms to exercise state sovereignty. Multiple sovereignties can be deemed to coexist in the same context. Digital sovereignty claims can therefore take the form not only of localisation law, but also of

legislation having an extraterritorial scope. From this perspective, the latter is not to be automatically condemned as imperialist because territorial boundaries are no longer the exclusive parameter to consider.

Looking forward, the development of internationally recognized standards for digital borders and cyber norms is essential. States, international organizations, and private-sector actors must work together to establish legal frameworks that balance state sovereignty, global interoperability, and human rights protections. Multi-stakeholder approaches, regional digital agreements, and mechanisms for incident attribution are likely to play a pivotal role in shaping future governance. Furthermore, investment in capacity-building for developing nations, transparency measures for technology companies, and harmonization of cybersecurity standards will strengthen global resilience against cybercrime and state-sponsored cyberattacks.

Ultimately, the future of digital sovereignty depends on cooperation, dialogue, and innovative legal solutions. By reconciling national interests with global principles, the international community can ensure that cyberspace remains secure, open, and equitable—allowing technology to serve as a bridge rather than a barrier between nations. The decisions made today will set the foundation for the legal and ethical framework governing the increasingly important and borderless domain of cyberspace.

References / Bibliography

https://www.orangecyberdefense.com/za/blog/research/digital-territory-and-sovereignty

https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/

https://www.geeksforgeeks.org/computer-networks/what-is-cyberspace/

https://en.wikipedia.org/wiki/Cyberspace

https://cyberjustice.blog/2019/07/17/china-the-great-firewall-cyber-sovereignty-freedom-of-speech-and-international-law/

https://en.wikipedia.org/wiki/Sovereign_Internet_Law

https://www.internetsociety.org/resources/internet-fragmentation/russias-sovereign-internet-law/

https://rimap.unhcr.org/node/62858#:~:text=Description,%2C%20arbitrary%20detention%2C%20and%20discrimination.

https://www.un.org/en/about-us/un-charter/full-text

https://en.wikipedia.org/wiki/Malabo_Convention

https://www.paloaltonetworks.com/cyberpedia/gdpr-compliance#:~:text=GDPR%20mandates%20explicit%20consent%20for,subject%2C%20not%20the%20data%20processor.

https://www.cio.com/article/188903/enabling-asean-s-digital-masterplan.html

https://www.basel.int/TheConvention/OpenendedWorkingGroup(OEWG)/OverviewandMandate/tabid/2295/Default.aspx

https://unidir.org/un-open-ended-working-group-and-unidir-side-events/

https://www.itu.int/en/about/Pages/default.aspx

https://en.wikipedia.org/wiki/International_Court_of_Justice

https://gdprlocal.com/digital-sovereignty/

https://cpl.thalesgroup.com/blog/encryption/data-sovereignty-privacy-governance

https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/12/rights-in-the-digital-age_d3a850de/deb707a8-en.pdf

https://blog.wamo.io/pros-and-cons-of-e-residency-in-estonia/

https://doras.dcu.ie/25498/1/Celeste_DigitalSovereigntyintheEU.pdf